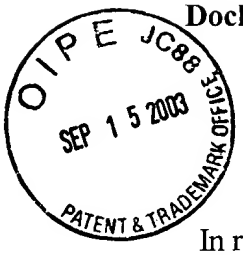
#9
9-26-03
PATENT
mel



Docket No. 00-022-MIS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **McCown et al.** §
§ Group Art Unit: **3621**
Serial No.: **09/598,777** §
§ Examiner: **Le, David Q.**
Filed: **June 16, 2000** §
§
For: **Method and System for Secure Credit Card Transactions** §
§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

Certificate of Mailing Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 09/11/03.
By: Amelia C. Nearing
Amelia C. Nearing

APPELLANT'S BRIEF (37 C.F.R. 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on July 11, 2003.

The fees required under § 1.17(c), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. 1.192(a))

REAL PARTIES IN INTEREST

The present application is assigned to Storage Technology Corporation, the real party in interest.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

Claims 1-40 stand finally rejected by the Examiner as noted in the final rejection mailed April 14, 2003.

STATUS OF AMENDMENTS

Applicant's Response to Final Office Action, transmitted on June 16, 2003, has been not entered.

SUMMARY OF INVENTION

Applicants claim a method, system, and product for securing a transaction in order to prevent fraudulent transactions. According to claim 1, a master key is received from a third party which stores a copy of the master key. The master key is kept secret and is not altered after a transaction.

According to an important feature of the present invention, a request for a digest is received from a requestor. This is an affirmative request. The claim states that a request for the digest is received. The master key and unique client information, which is associated with the master key, are then retrieved. The requested digest is then created by hashing the unique client

information and the master key. The digest along with the client information is returned to the requestor to be used for transacting with a third party.

According to claim 8, a smart card is initialized by receiving within the card a secret master key from a credit card issuer which remains known to the credit card issuer. Again the master key is kept secret. The smart card receives a transaction from a merchant which includes unique merchant information and a request for a billing digest. Unique client information is retrieved from the smart card memory and the master key is retrieved. The billing digest is created by hashing the unique client information, the master key, and the merchant information that was received from the merchant. The billing digest, merchant information, and client information are then passed to the requestor.

According to claim 11, a smart card is initialized by receiving a master key from a credit card issuer. A data transmission is sent to the smart card which includes merchant information and a request for a billing digest. The billing digest, merchant information, and client information are received from the smart card. The billing digest is hashed from the merchant information, client information, and master key from the smart card. The merchant information and client information are transmitted from the smart card to the credit card issuer.

According to claim 13, a master key is received from a third party. The master key is secret and remains unchanged and not altered after a transaction. The third party stores a copy of the master key within the third party. The third party receives a transaction request from a requestor. The request includes a digest and unique client information. The master key is associated with client information that was received by the third party from the requestor. The copy of the master key is accessed based on the unique client information. An authorization digest is created by hashing the client information and the copy of the master key. The third party compares the authorization digest with the digest from the requestor. A response is returned to the requestor from the third party based on the outcome of the comparison.

According to claim 20, a billing digest is generated within a customer's smart card. The billing digest is hashed from merchant information, customer information, and a secret master key. A master key is received from a credit card issuer when the smart card is initialized by the credit card issuer. The master key is associated with the customer information. An authentication digest is created by the credit card issuer which is hashed from the merchant information, customer information, and a master key that is associated with the customer

information. The authorization digest is compared with the billing digest. A transaction is authorized based on the comparison.

According to claim 21, a master key is indexed to an account identifier for an account which is between a customer and a financial institution. The master key is provided to the financial institution and a smart card controlled by the customer. Transaction data is passed through a third party that includes the customer account identifier, third party information, and a billing digest. The billing digest is created from the customer account identifier, the third party information, and the master key.

According to claim 22, a master key is received upon initialization of a smart card from a third party. A digest is created from financial account information and the master key. The digest and the financial account information are transmitted to a requestor for approval by the third party.

According to claim 23, a smart card creates a billing digest from resident client information, a resident master key, and imported merchant information. The secret master key is received from a financial institution upon initialization of the smart card. The master key remains unchanged after use of the smart card and is kept secret. The master key is associated with the resident client information. A merchant system is included for requesting the billing digest. The merchant system also passes secure transaction information and the billing digest to the financial institution. The transaction information includes client information and the imported merchant information. The financial institution receives the transaction information and billing digest and authorizes a transaction by accessing a master key stored within the financial institution based on the client information, creates an authorization digest and compares the authorization digest to the billing digest.

According to claim 24, a master key is received from a third party prior to a transaction which is kept secret and remains unchanged after the transaction. A request for a digest is received from a requestor. A master key and client information are retrieved. The master key is associated with the retrieved client information. The digest is created by hashing the client information and the master key. The digest and client information are returned to the requestor to be used for transacting with the third party.

According to claim 32, a master key is provided to a client from a third party. The key remains unchanged after a transaction. A request is received from a requestor which includes a

digest and client information. The digest is created using the master key provided to the client and the client information. The master key is associated with the client information. The third party accesses the master key that is stored in the third party using the client information. An authorization digest is created by hashing the client information and the master key. The authorization digest and digest from the requestor are compared and a response is returned to the requestor based on the outcome of the comparison.

ISSUES

Is the Examiner's rejection of claims 1-2, 5, 7-8, and 11-12 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 5,850,442 issued to *Muftic*; and the rejection of claims 3, 6, 9-10, 13-14, 17-26, 28-33, and 36-40 under 35 U.S.C. § 103(a) as being unpatentable over *Muftic*; and the rejection of claims 4, 9, 15-16, 27, and 34-35 under 35 U.S.C. § 103(a) as being unpatentable over *Muftic* in view of U.S. Patent 5,931,917 issued to *Nguyen* well founded?

GROUPING OF CLAIMS

For the purposes of this appeal, claims 1-40 stand or fall together as one group.

ARGUMENT

Applicant's claims are believed to be patentable over the prior art because the prior art, neither singly nor in combination, describes, teaches, or suggests: (1) an affirmative request being made for a digest; (2) transmitting a digest; (3) receiving a request for a digest from a requestor where the digest and client information are then returned to the requestor for transacting with a third party; (4) a secret master key being obtained from a third party prior to a transaction where the third party stores a copy of this same master key; (5) unique client information being associated with the master key; or (6) unique merchant information being used to access the master key.

The Examiner rejected claims 1-2, 5, 7-8, and 11-12 under 35 U.S.C. § 102(b) as being

anticipated by U.S. Patent 5,850,442 issued to *Muftic*. This position is not well founded.

Applicants' claim 1 describes receiving a request for a digest. This is an affirmative step that must be taught in *Muftic* in order for *Muftic* to anticipate Applicants' claims. *Muftic* describes a message digest at column 2, lines 25-51. Nowhere else is *Muftic* are digests discussed. *Muftic* teaches that digests may be created in order to act as an additional verification that data has not been altered since the digest was created. "A message digest of the document is analogous to a cyclic redundancy code (CRC) check sum attached to the end of a packet."

Muftic teaches that a document or a digest can be signed by encrypting either the document or a digest with a private key. Column 2, lines 15-51. Thus, according to *Muftic*, "signing" a document does not mean providing a digest. "Signing" a document merely means to encrypt the document with a key of some sort.

Throughout the rest of *Muftic*, digests are not discussed. *Muftic* does describe in several places signing an order form or check and then transmitting the signed form. However, *Muftic* does not describe requesting a digest, and then transmitting that digest. Transmitting a signed form is not the same as requesting a digest and then transmitting that digest. Further, *Muftic* teaches that a document may be signed without creating a digest. Thus, when *Muftic* teaches that a signed document may be transmitted, *Muftic* is not necessarily teaching that a digest is being transmitted at all.

Muftic does not describe, teach, or suggest receiving a request for a digest. As described by the reference, digests may be, but are not necessarily, generated and then appended to a document as CRC-type check sums. Requests are not made for the digest itself. The digest is just automatically added as a check sum when that type of signature is used. *Muftic* does not describe the affirmative step of receiving a request for a digest. Therefore, *Muftic* does not anticipate Applicants' claims.

The Examiner refers to column 2, lines 27-51 and Figure 10, step 1030 as teaching the step of receiving a request for a digest. As discussed above, column 2, lines 27-51 teaches only the existence and typical use of a digest. Column 2, lines 27-52, does not teach receiving a request for a digest. Figure 10, step 1030 describes receiving an order form from a homepage server. Figure 10 describes an order form that is received from a vendor. Figure 10 does not describe the vendor sending a request for a digest. In figure 10, the vendor sends information, not requests for digests.

Figure 10 teaches merely that an order form may be filled in, signed, and then returned. Returning a signed order form does not teach either (1) requesting a digest, or (2) transmitting a digest since the process of signing an order form does not teach digests.

Applicants' claim 1 also describes the request for the digest being received from a requestor. A master key is received from a third party. A digest is created using unique client information and the master key. The digest and the unique client information are then returned to the requestor. The digest and unique client information will be used for transacting with the third party.

Muftic does not teach returning a digest and unique client information to a requestor that will be used for transacting with the third party that supplied the master key.

Applicants describe retrieving a master key that was received from a third party, and that remains unchanged and kept secret. Applicants' claims describe a copy of the master key being stored by the third party. The Examiner states that *Muftic* teaches retrieving a master key in Figure 10, step 1060. This step of *Muftic's* figure 10 states, "Digitally sign order form, create digital envelope and send to server." The accompanying text, at column 13, lines 36-39, states, "The user digitally signs the order form and sends it to the server or directly to the vendor as specified in information contained on the server (1060)." This section of *Muftic* does not refer to a master key or any other type of key. This section of the reference certainly does not describe a master key that was received from a third party and that remains unchanged and kept secret. This section of the reference does not describe a copy of the master key being stored by the third party.

The Examiner states that Figure 16 teaches a secret master key by teaching a smart token or certificate. Figure 16 states that an electronic charge slip with issuer and account number filled in is displayed. A user may then fill in the electronic ID of the seller and the amount. A digital signature is applied. The change slip is transferred to the seller's computer and a copy is stored. The electronic receipt, optionally signed by the seller, is returned. The account unpaid balance is increased and the process ends.

Nothing in this description describes a master secret key that is obtained from a third party prior to a transaction where the key remains unchanged and is kept secret, and where the third party keeps a copy of the key.

Applicants' claim 8 describes receiving within a smart card a request from a merchant for a billing digest. The Examiner states that the reference describes this step at column 2, lines 15-

51 and figure 10, step 1030. Specifically, the Examiner refers to an order form that is received. Applicants, however, do not claim receiving an order form. Applicants claim a smart card that receives a request from a merchant for a billing digest. *Muftic* does not describe, teach, or suggest a smart card that receives a request from a merchant for a billing digest. *Muftic's* figure 10 describes a user logging on to a home page server, obtaining an order form from the server, filing out the order form, and digitally signing the order form. Nothing in this section of *Muftic*, describes a smart card receiving a request for a digest from a merchant. Figure 10 describes a merchant supplying information to a user. Figure 10 does not describe a merchant sending a request to a user. Figure 10 does not describe a smart card receiving a request from a merchant for a digest.

Applicants' claim 11 similarly describes sending a data transmission to a smart card including unique merchant information and a request for a billing digest. As discussed above, *Muftic* does not describe, teach, or suggest a request for a billing digest.

Applicants' claims describe receiving a secret master key from a third party that remains unchanged and is not altered after the transaction. The third party stores a copy of the master key. *Muftic* teaches public key encryption. However, nothing in *Muftic* explicitly states that a master key is received from a third party that keeps a stored copy where the key remains unchanged and is not altered after the transaction. In public key encryption, typically data is encrypted with one key and decrypted with another. Thus, the decryptor does not have a copy of the key used to encrypt the data.

Muftic does describe a session key that is changed after each transaction. However, this key continually changes. It does not remain unchanged. See column 2, line 63 through column 3, line 2. *Muftic* does not teach a master key that is received from a third party that keeps a stored copy where the key remains unchanged and is not altered after the transaction.

The Examiner rejected claims 3, 6, 9-10, 13-14, 17-26, 28-33, and 36-40 under 35 U.S.C. § 103(a) as being unpatentable over *Muftic*. This position is not well founded.

Applicants' claim 3 describes the request for a digest including unique merchant information which is used to access the master key. The Examiner states that it would be obvious to include unique merchant information that would dictate which master key the client system should use. However, this is not what is claimed by Applicants. Applicants claim a request for a digest received from a requestor including unique merchant information which is

used to access a master key that was received from a third party where the third party keeps a copy of the master key.

It is not clear where the merchant information suggested by the Examiner should be included. There is no request for a digest from a requestor in which to include the merchant information. The Examiner had described the request for a digest as being an order form as described by *Muftic's* figure 10, step 1030. This order form is downloaded from a vendor, completed by the user, and then sent back to that same vendor. Thus, the merchant information suggested by the Examiner would be added to an order form that is completed by the user and then supplied back to the merchant. *Muftic* does not describe, teach, or suggest adding merchant information to an order form that was originally retrieved from the merchant, completed, and then supplied back to the merchant. *Muftic* does not provide any teaching as to why a merchant would want to supply merchant information to a user that would then just send that same merchant information back to the merchant.

Applicants' claim 13 describes the master key being associated with client information. The Examiner states that this is taught referring to his comments regarding claims 1, 8, and 11. The Examiner's comments describe Figure 16 which states that an electronic charge slip with issuer and account number filled in is displayed. A user may then fill in the electronic ID of the seller and the amount. A digital signature is applied. The change slip is transferred to the seller's computer and a copy of stored. The electronic receipt, optionally signed by the seller, is returned. The account unpaid balance is increased and the process ends.

As discussed above, nothing in this description describes a master secret key that is obtained from a third party prior to a transaction where the key remains unchanged and is kept secret, and where the third party keeps a copy of the key. Further, nothing describes a master key that is associated with client information. Claim 13 also describes the client information being received by a third party from a requestor. Nothing in *Muftic* describes a master key that is associated with client information that was received from a third party by a requestor.

Applicants' claim 23 describes a merchant system that requests a digest. As described above, nothing in *Muftic* describes a request for a digest. Further, nothing in *Muftic* describes a merchant system that requests a digest.

The Examiner rejected claims 4, 9, 15-16, 27, and 34-35 under 35 U.S.C. § 103(a) as being unpatentable over *Muftic* in view of U.S. Patent 5,931,917 issued to *Nguyen*. This position is not

well founded.

Muftic and *Nguyen* in combination do not describe, teach, or suggest receiving a request for a digest from a requestor where the digest is created using unique client information that includes a reference number provided to a client by a third party.

Applicant's claims are believed to be patentable over the prior art because the prior art, neither singly nor in combination, describes, teaches, or suggests: (1) an affirmative request being made for a digest; (2) transmitting a digest; (3) receiving a request for a digest from a requestor where the digest and client information are then returned to the requestor for transacting with a third party; (4) a secret master key being obtained from a third party prior to a transaction where the third party stores a copy of this same master key; (5) unique client information being associated with the master key; or (6) unique merchant information being used to access the master key.

Lisa L.B. Yociss
Reg. No. 36,975
Carstens, Yee & Cahoon, LLP
PO Box 802334
Dallas, TX 75380
(972) 367-2001

APPENDIX OF CLAIMS

The text of the claims involved in the appeal reads:

1. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key;

receiving a request for a digest from a requestor;

retrieving the master key;

retrieving unique client information;

the client information being associated with the master key;

creating the digest by hashing the unique client information and the master key; and

returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the third party.

2. The method recited in claim 1 above, wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information.

3. The method recited in claim 1 above, wherein the request includes unique merchant information which is used to access the master key.

4. The method recited in claim 1 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

5. The method recited in claim 1 above, wherein creating the digest by hashing is performed by a smart card.

6. The method recited in claim 1 above further comprises encrypting the unique client information prior to retrieving the unique client information.

7. The method recited in claim 1 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

8. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card by receiving within the card a secret master key from a credit card issuer, the master key being kept secret;

receiving, into the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving unique client information, from the smart card memory;

retrieving the master key, the master key being known to the credit card issuer;

creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing the billing digest, the unique merchant information and the unique client information to the requestor.

9. The method recited in claim 8 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the credit card issuer.

10. The method recited in claim 8 above further comprises encrypting the unique client information and the unique merchant information prior to passing the information to the merchant.

11. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card by receiving within the card a secret master key from a credit card issuer, the master key being kept secret;

sending a data transmission to the smart card, wherein the data transmission includes unique merchant information and a request for a billing digest;

receiving the billing digest, the unique merchant information and unique client information from the smart card, the billing digest being hashed from the unique merchant information, unique client information and the master key from the smart card; and

transmitting the unique merchant information and unique client information from the smart card to a credit card issuer.

12. The method recited in claim 11 above further comprises receiving a response from the credit card issuer.

13. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged, and is not altered after the transaction, the third party storing a copy of the master key within the third party, the master key being kept secret;

receiving, by the third party, a transaction request from a requestor, wherein the request includes a digest and unique client information;

the client information being associated with the master key;

accessing the copy of the master key based on the unique client information;

creating an authorization digest by hashing the unique client information and the copy of the master key;

comparing, by the third party, the authorization digest with the digest from the requestor; and

returning a response to the requestor from the third party, the content of the response being based on an outcome of the comparison of the authorization digest with the digest from the requestor.

14. The method recited in claim 13 above, wherein the request includes unique requestor information and creating the authorization digest further comprises hashing the unique requestor information.

15. The method recited in claim 13 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

16. The method recited in claim 15 above further comprises:

accessing all previously used reference numbers associated with the unique client information;

comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information.

17. The method recited in claim 13 above, wherein creating the authentication digest by hashing is performed by a smart card.

18. The method recited in claim 13 above further comprises decrypting the unique client information prior accessing the master key.

19. The method recited in claim 13 above, wherein the third party is a credit card issuer, the transaction is a credit card transaction and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

20. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

generating a billing digest in a customer's smart card, the billing digest being hashed from merchant information, customer information and a secret master key;

receiving the master key from a credit card issuer upon an initialization of the smart card by the credit card issuer, the master key being associated with the customer information;

creating an authentication digest by the credit card issuer, wherein the authentication digest is hashed from the merchant information, customer information and a master key associated with the customer information;

comparing the authorization digest with the billing digest; and

authorizing a transaction based on the comparison of the authorization digest with the billing digest.

21. A method for securing a transaction comprising:

indexing a secret master key to an account identifier for an account, wherein the account is between a customer and a financial institution;

providing the master key to the financial institution and a smart card controlled by the customer;

passing transaction data through a third party, wherein the transaction data includes at least the customer account identifier, third party information and a billing digest which is created from the customer account identifier, the third party information and the master key.

22. A smart card for conducting secure transactions in order to prevent fraudulent transactions comprising:

a input/output mechanism;

a processor; and

a memory containing:

financial account information;

a secret master key received upon initialization of the smart card, the master key remaining unchanged throughout the use of the smart card, the master key being received from a third party;

functional hashing algorithm;

an executable application, for executing on the processor, for invoking the functional hashing algorithm, wherein the functional hashing algorithm creates a digest from the financial account information and the master key and further wherein the executable application transmits, via the input/output mechanism, the digest and the financial account information to a requestor for approval by the third party.

23. A system for conducting secure transactions in order to prevent fraudulent transactions comprising:

a client smart card for creating a billing digest from a resident client information, a resident secret master key and imported merchant information;

the master key being received from a financial institution upon initialization of the smart card, the master key remaining unchanged after use of the smart card, the master key being kept secret, and the master key being associated with the resident client information;

a merchant system for requesting the billing digest and for passing secure transaction information and the billing digest to the financial institution, wherein the transaction information comprises the client information, and the imported merchant information; and

the financial institution for receiving the transaction information and billing digest and for authorizing a transaction by:

accessing a master key stored within the financial institution based on the client information;

creating an authorization digest from the master key stored in the financial institution , the client information and the merchant information; and

comparing the authorization billing digest with the billing digest.

24. A system for securing a transaction in order to prevent fraudulent transactions comprising:

receiving means for receiving a secret master key from a third partition prior to the transaction, the master key remaining unchanged after the transaction, the master key being kept secret;

receiving means for receiving a request for a digest from a requestor;

retrieving means for retrieving the master key;

retrieving means for retrieving unique client information;

the client information being associated with the master key;

creating means for creating the digest by hashing the unique client information and the master key; and

returning means for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the third party.

25. The system recited in claim 24 above, wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information.

26. The system recited in claim 24 above, wherein the request includes unique merchant information which is used to access the master key.

27. The system recited in claim 24 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

28. The system recited in claim 24 above, wherein the creating means for creating the digest by hashing is performed by a smart card.

29. The system recited in claim 24 above further comprises encrypting means for encrypting the unique client information prior to returning the unique client information.

30. The system recited in claim 24 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

31. The system recited in claim 24 above further comprises:

fingerprint reading and identification means for reading a fingerprint and authorizing a client based on an identity of a client's fingerprint.

32. A system for securing a transaction in order to prevent fraudulent transactions comprising:

providing means for providing from a third party a secret master key to a client, the master key remaining unchanged after the transaction;

receiving means for receiving a transaction request from a requestor, wherein the request includes a digest and unique client information, the digest being created utilizing the master key provided to the client and the unique client information;

the unique client information being associated with the master key;

accessing means for accessing, by the third party, a master key stored within the third party based on the unique client information;

creating means for creating an authorization digest by hashing the unique client information and the master key;

comparing means for comparing the authorization digest with the digest from the requestor; and

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the authorization digest with the digest from the requestor.

33. The system recited in claim 32 above, wherein the request includes unique requestor information and creating the authorization digest further comprises hashing the unique requestor information.

34. The system recited in claim 32 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

35. The system recited in claim 34 above further comprises:

accessing means for accessing all previously used reference numbers associated with the unique client information;

comparing means for comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information.

36. The system recited in claim 32 above, wherein creating the authentication digest by hashing is performed by a smart card.

37. The system recited in claim 32 above further comprises decrypting the unique client information prior accessing the master key.

38. The system recited in claim 32 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

39. A computer program product for securing a transaction in order to prevent fraudulent transactions embodied on a computer readable medium comprising:

providing instructions for providing from a third party a secret master key, the master key remaining unchanged after the transaction;

receiving instructions for receiving a request for a digest from a requestor;

retrieving instructions for retrieving the master key;

retrieving instructions for retrieving unique client information;

the master key being associated with the client information;

creating instructions for creating the digest by hashing the unique client information and the master key; and

returning instructions for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the third party.

40. A computer program product for securing a transaction in order to prevent fraudulent transactions embodied on a computer readable medium comprising:

initializing instructions for initializing a smart card by receiving within the card a secret master key from a credit card issuer;

receiving instructions for receiving, into the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving instructions for retrieving unique client information, from the smart card memory;

the unique client information being associated with the master key;

retrieving instructions for retrieving the master key, the master key being provided by the credit card issuer;

creating instructions for creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing instructions for passing the billing digest, the unique merchant information and the unique client information to the requestor.